Data Communication and Net-Centric Computing

COSC 1111/2061/1110

Lecture 2

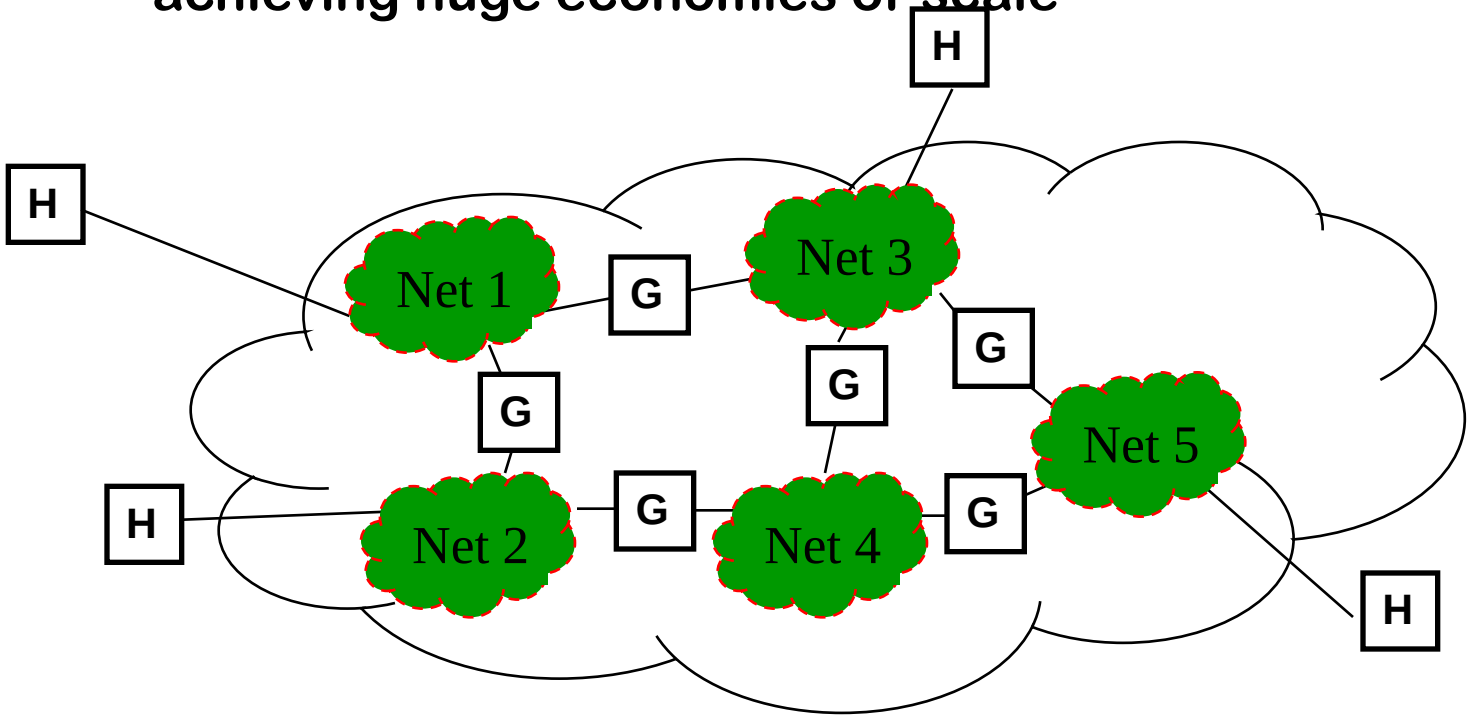
Internetworking, IPv4, IPv6

Lecture Overview

- During this lecture, we will understand
  - The principles of Internetworking
  - Look at Internet Protocols
  - IPv4/ IPv6
- Recommended reading
  - Chapters 18 and 19 (Stallings)

Why Internetworking?

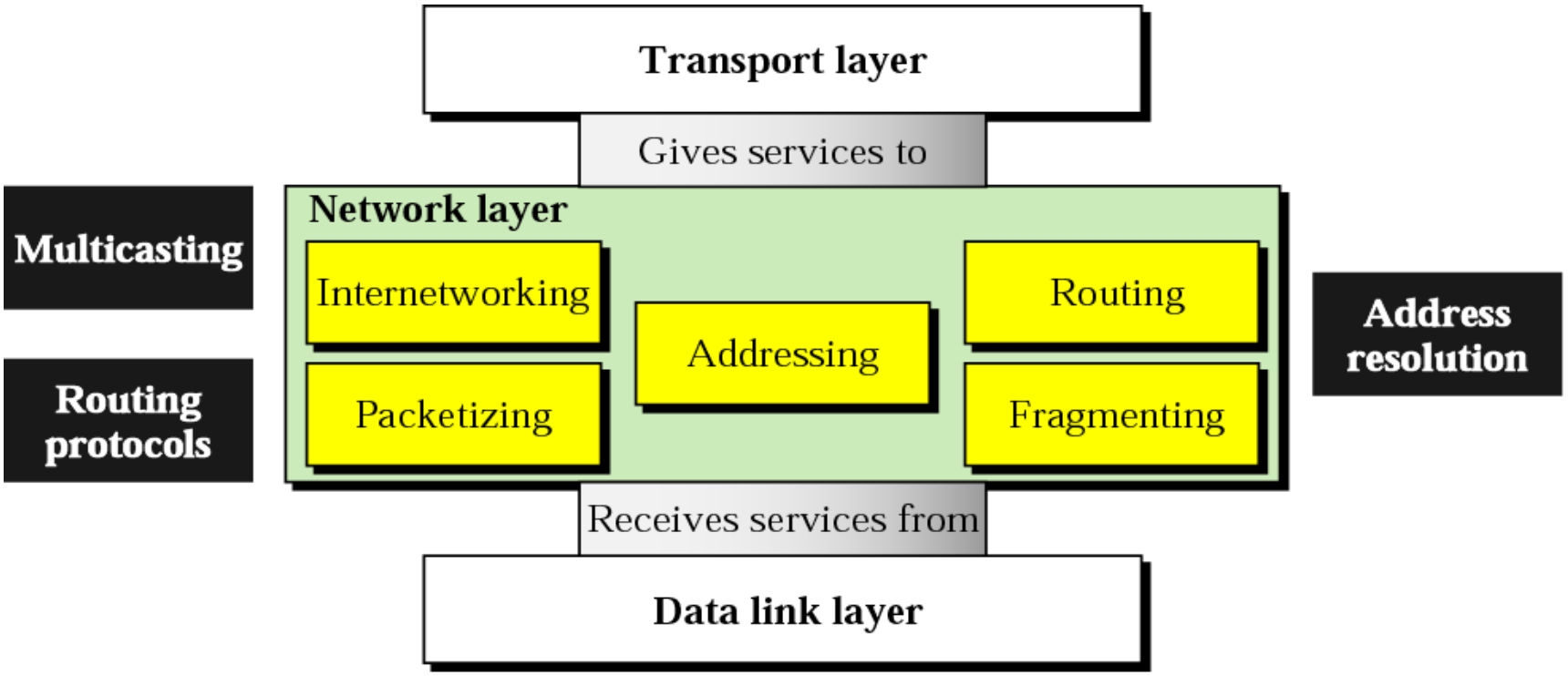
- To build a "network of networks" or internet
  - operating over multiple, coexisting, different network technologies
  - providing ubiquitous connectivity through IP packet transfer
  - achieving huge economies of scale



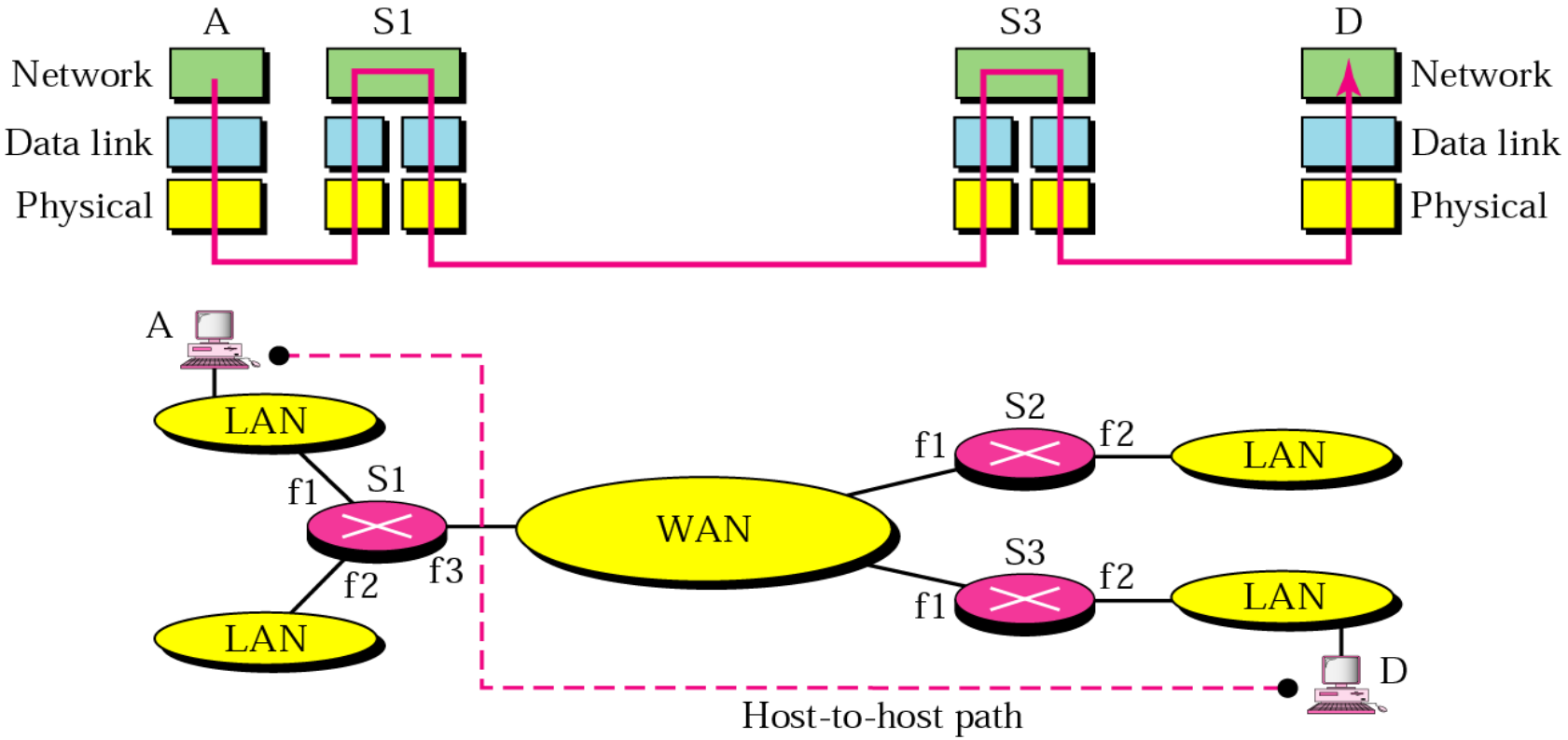
Why Internetworking?

- To provide *distributed applications*
  - Any application designed to operate based on Internet communication services immediately operates across the entire Internet
  - Rapid deployment of new applications
    - Email, WWW, Peer-to-peer
  - Applications independent of network technology
    - New networks can be introduced below
    - Old network technologies can be retired

Position of network layer



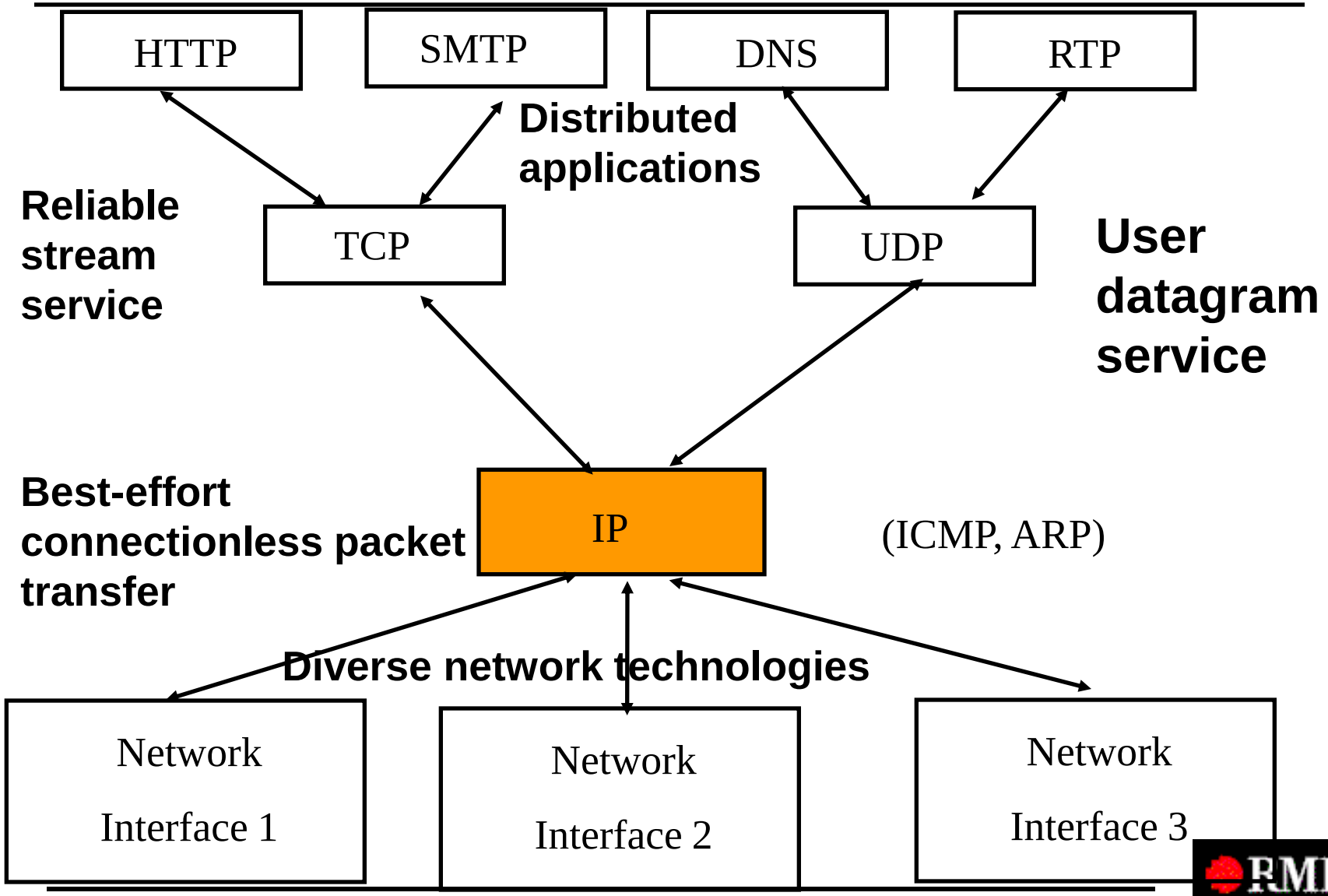
Network layer in an internetwork



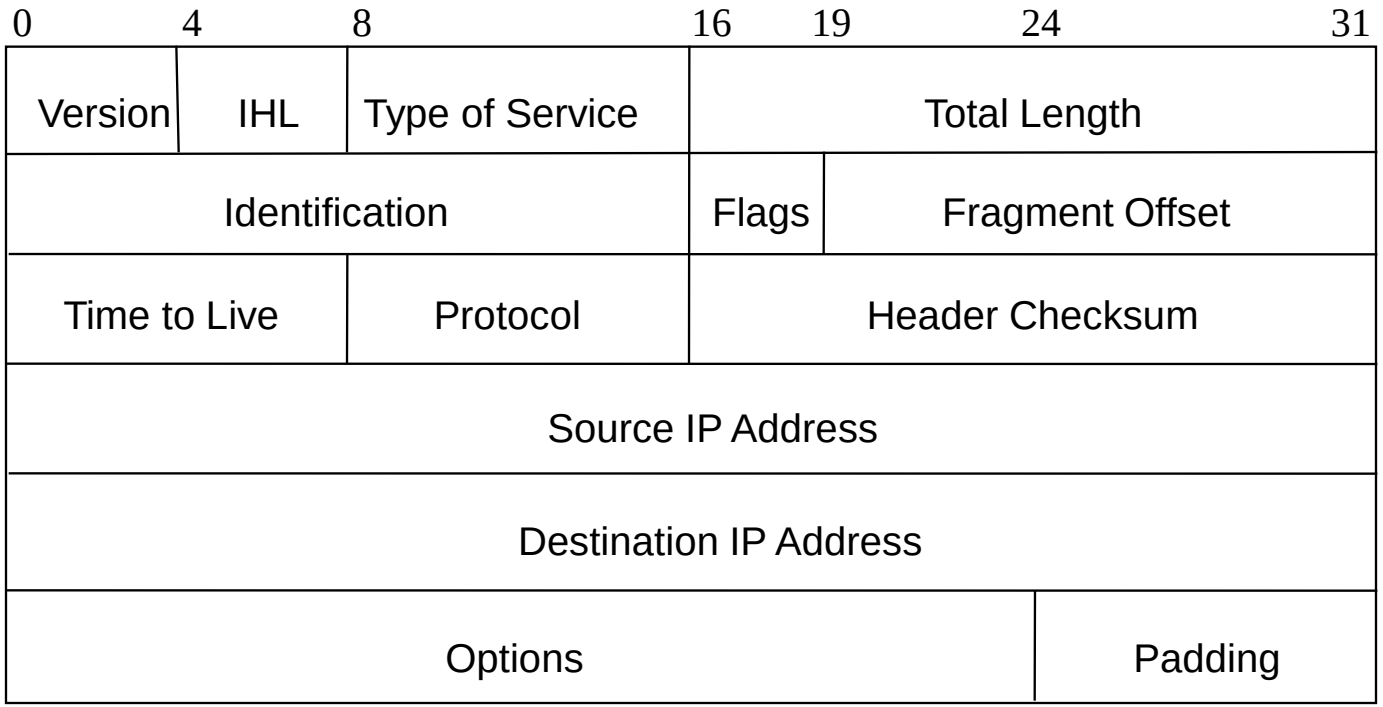
Internet Protocol

- Provides best effort, connectionless packet delivery
  - motivated by need to keep routers simple and by adaptability to failure of network elements
  - packets may be lost, out of order, or even duplicated
  - higher layer protocols must deal with these, if necessary
- RFCs 791, 950, 919, 922, and 2474.
- IP is part of Internet STD number 5, which also includes:
  - Internet Control Message Protocol (ICMP), RFC 792
  - Internet Group Management Protocol (IGMP), RFC 1112

TCP/IP Protocol Suite

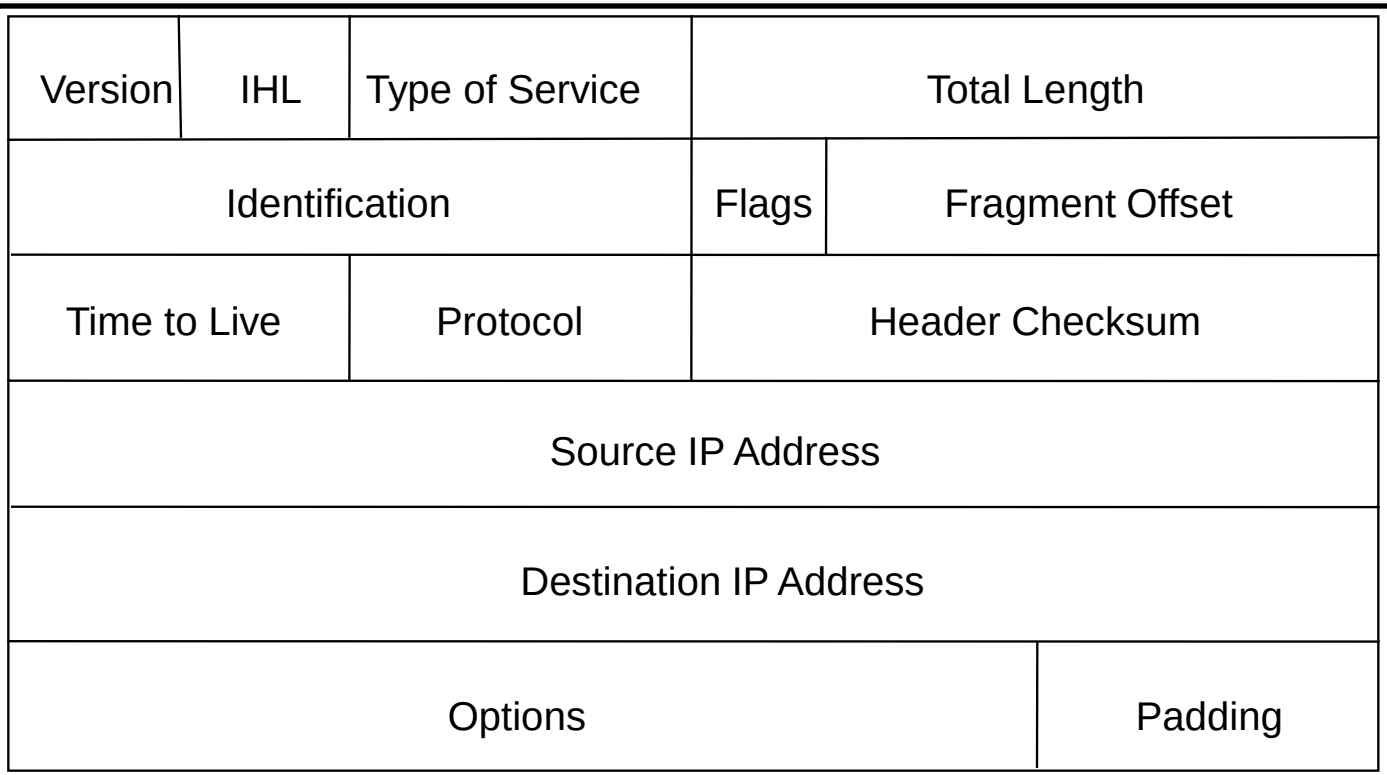


IP Packet Header



- Minimum 20 bytes
- Up to 40 bytes in options fields

IP Packet Header

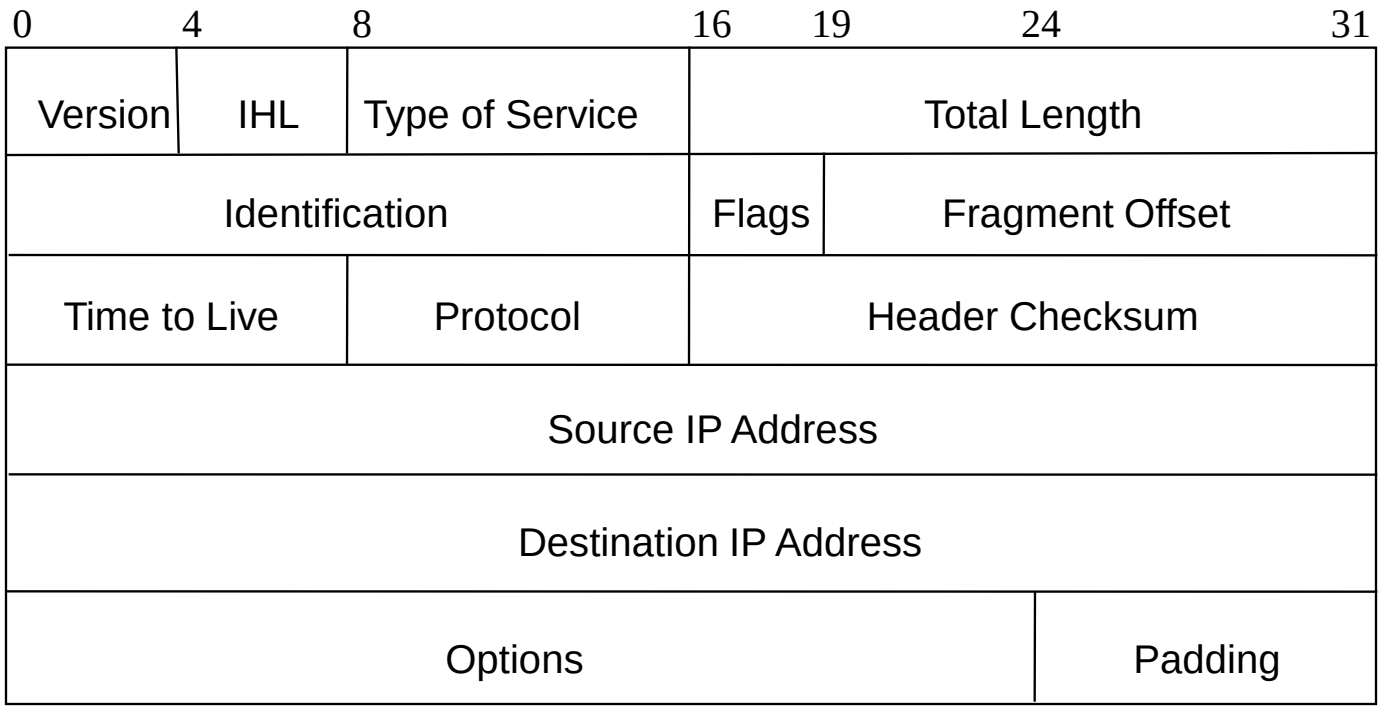


Version: current IP version is 4.

Internet header length (IHL): length of the header in 32-bit words.

Type of service (TOS): traditionally priority of packet at each router. Recent Differentiated Services redefines TOS field to include other services besides best effort.

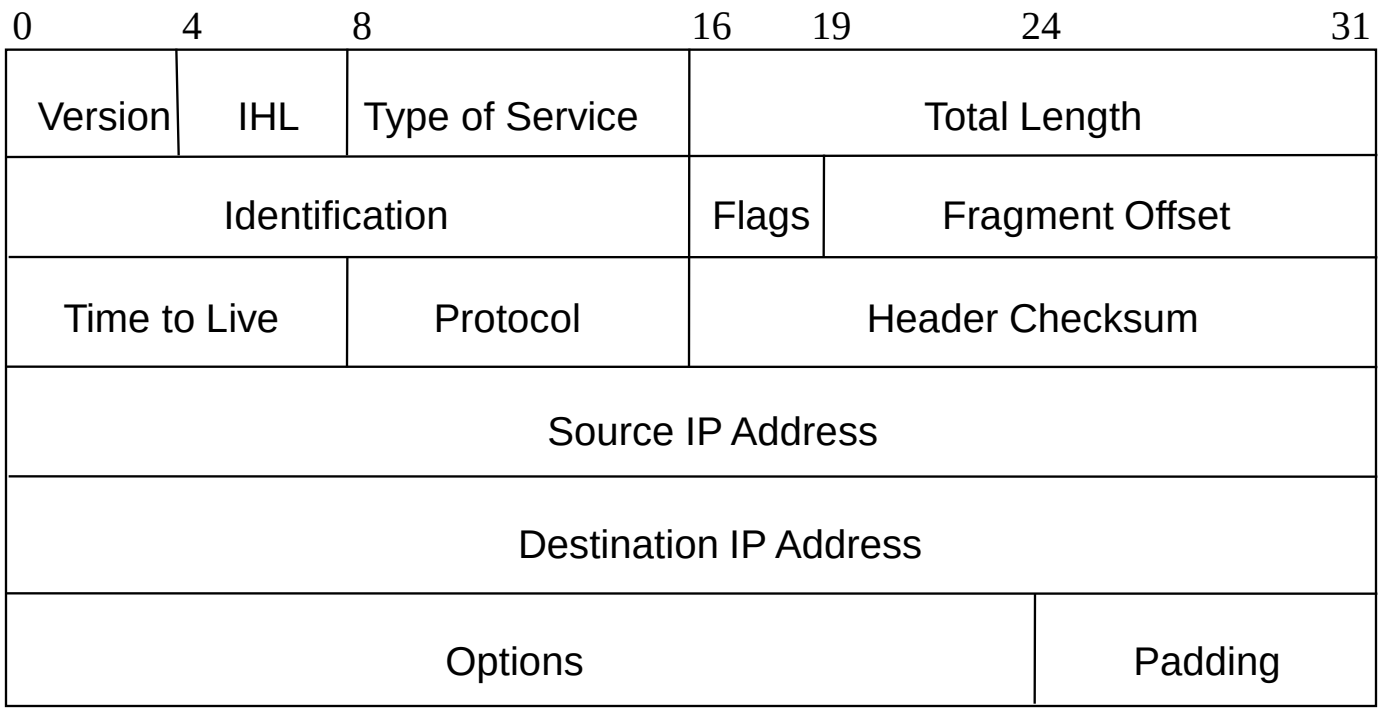
IP Packet Header



Total length: number of bytes of the IP packet including header and data, maximum length is 65535 bytes.

Identification, Flags, and Fragment Offset: used for fragmentation and reassembly.

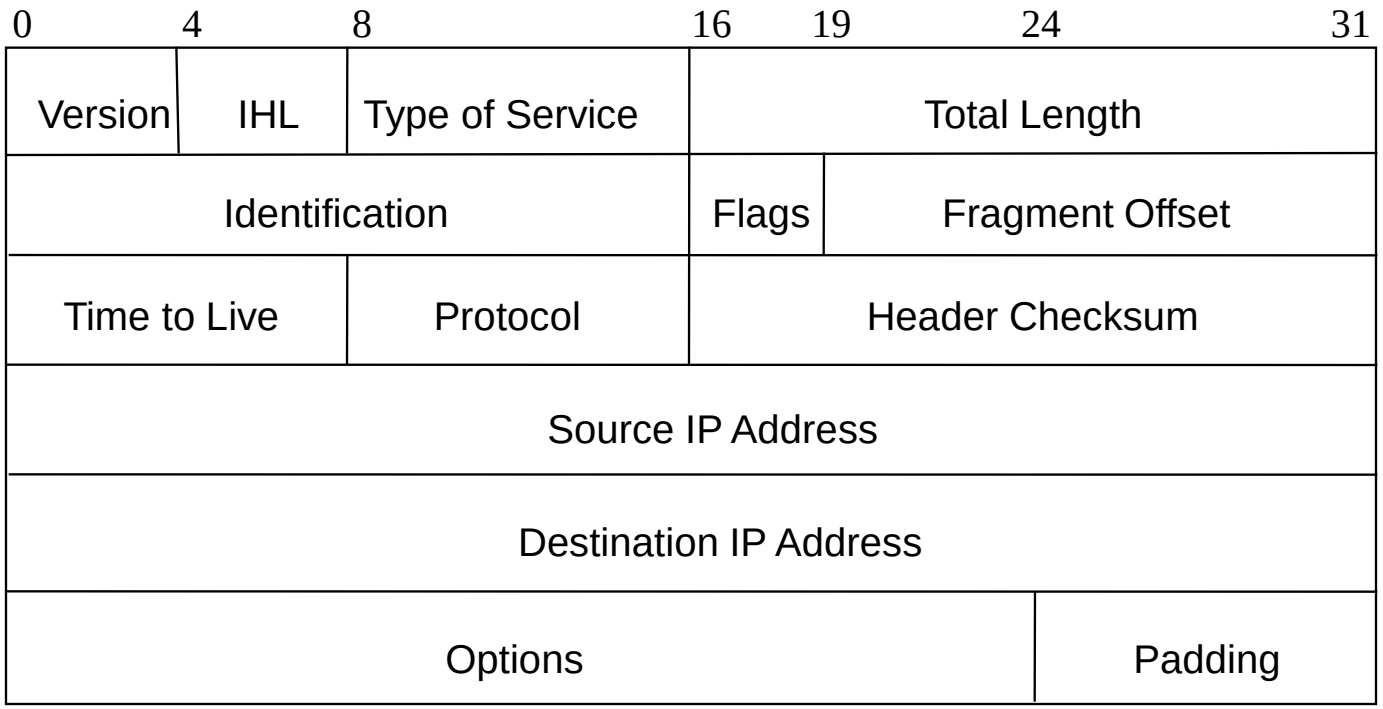
IP Packet Header



Time to live (TTL): number of hops packet is allowed to traverse in the network.

- Each router along the path to the destination decrements this value by one.
- If the value reaches zero before the packet reaches the destination, the router discards the packet and sends an error message back to the source.

IP Packet Header

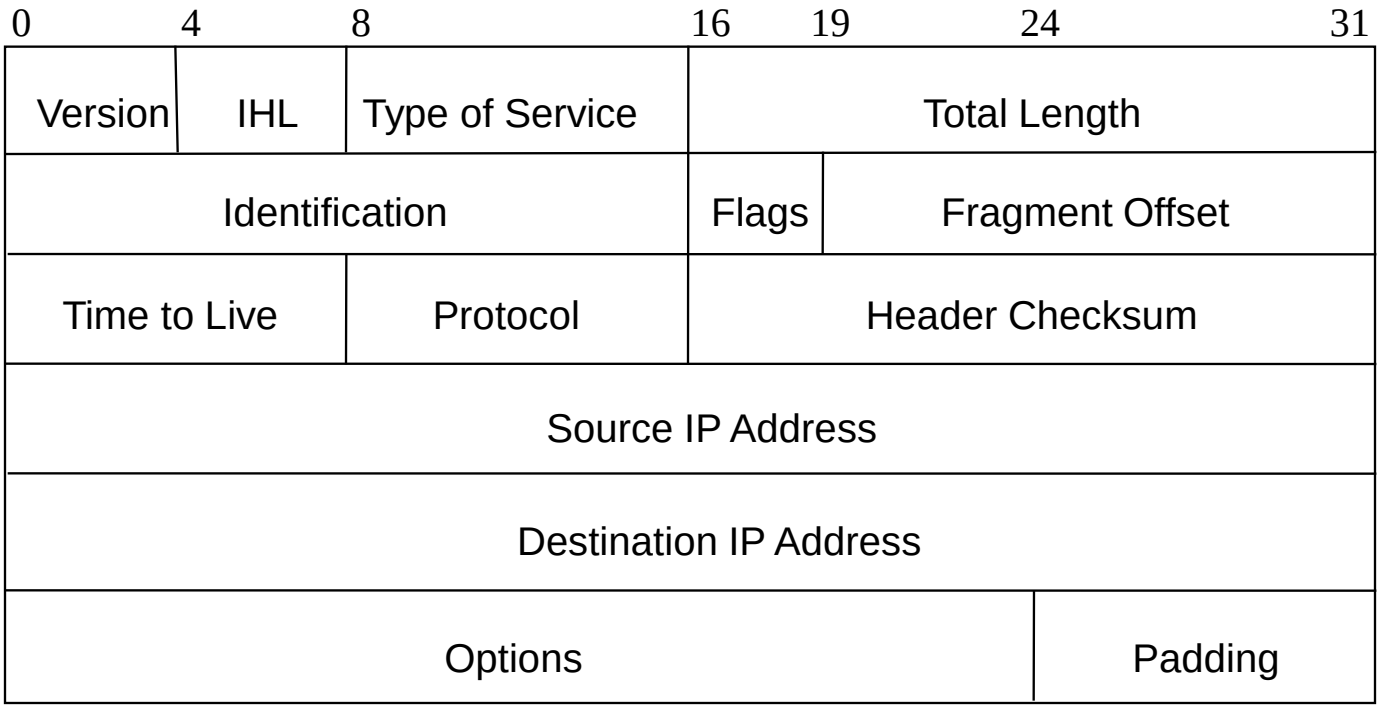


Protocol: specifies upper-layer protocol that is to receive IP data at the destination. Examples include TCP (protocol = 6), UDP (protocol = 17), and ICMP (protocol = 1).

Header checksum: verifies the integrity of the IP header.

Source IP address and **destination IP address:** contain the addresses of the source and destination hosts.

IP Packet Header

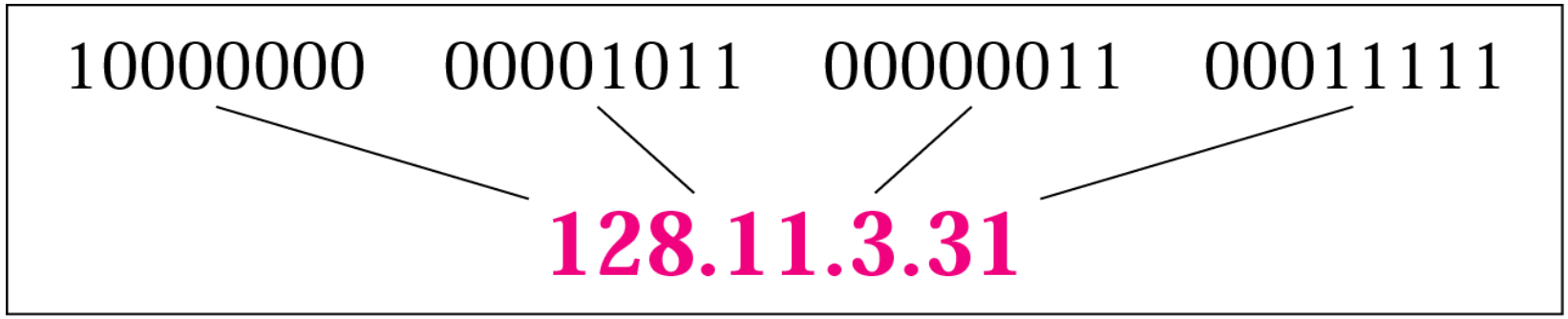


Options: Variable length field, allows packet to request special features such as security level, route to be taken by the packet, and timestamp at each router. Detailed descriptions of these options can be found in [RFC 791].

Padding: This field is used to make the header a multiple of 32-bit words

Dotted-decimal/binary notation

- An IP address is a 32-bit address
- The IP addresses are unique and universal



Binary-decimal conversion

Example 1

Change the following IP addresses from binary notation to dotted-decimal notation.

a. **10000001 00001011 00001011 11101111**

b. **11111001 10011011 11111011 00001111**

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation:

a. **129.11.11.239**

b. **249.155.251.15**

Decimal-binary conversion

Example 2

Change the following IP addresses from dotted-decimal notation to binary notation.

a. **111.56.45.78**

b. **75.45.34.78**

Solution

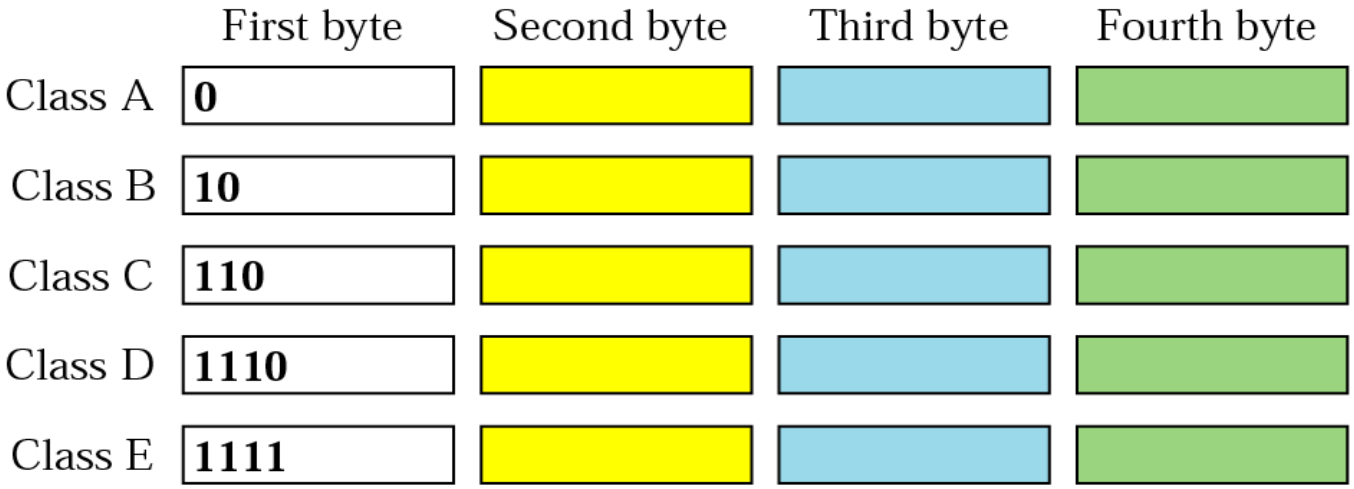
We replace each decimal number with its binary equivalent:

a. **01101111 00111000 00101101 01001110**

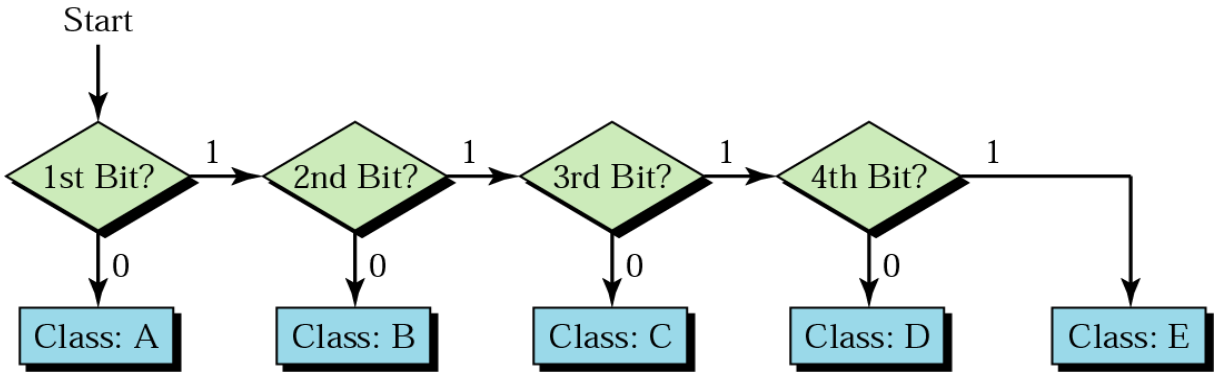
b. **01001011 00101101 00100010 01001110**

IPv4 Address Formats

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.



Finding the address class



Finding the address class -Example

Example 3

Find the class of each address:

a. **0**0000001 00001011 00001011 11101111

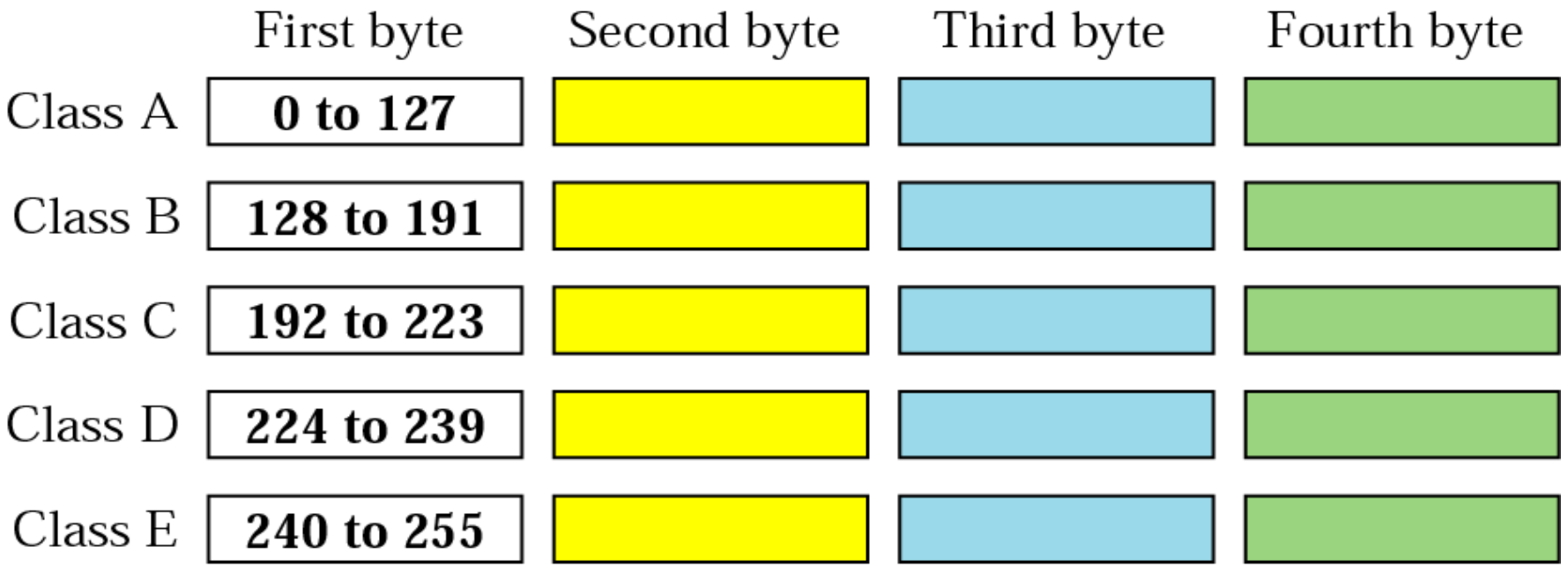
b. **1111**0011 10011011 11111011 00001111

Solution

a. The first bit is 0; this is a class A address.

b. The first 4 bits are 1s; this is a class E address.

Finding the class in decimal notation



Finding the address class -Example

Example 4

Find the class of each address:

a. **227**.12.14.87

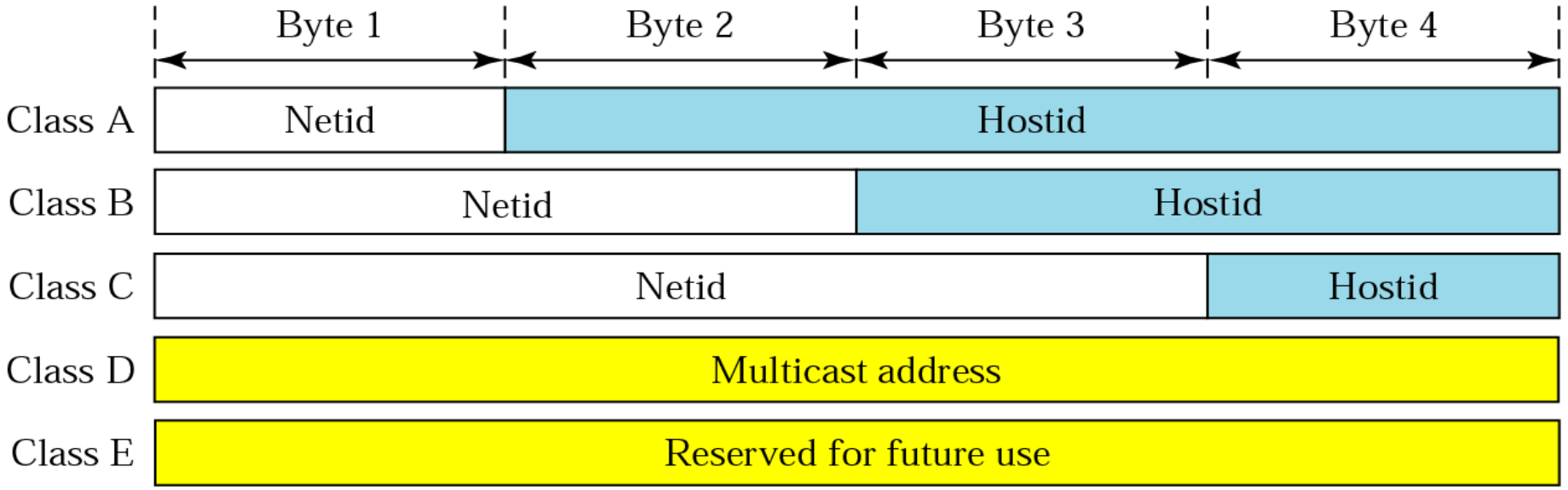
b. **252**.5.15.111

c. **134**.11.78.56

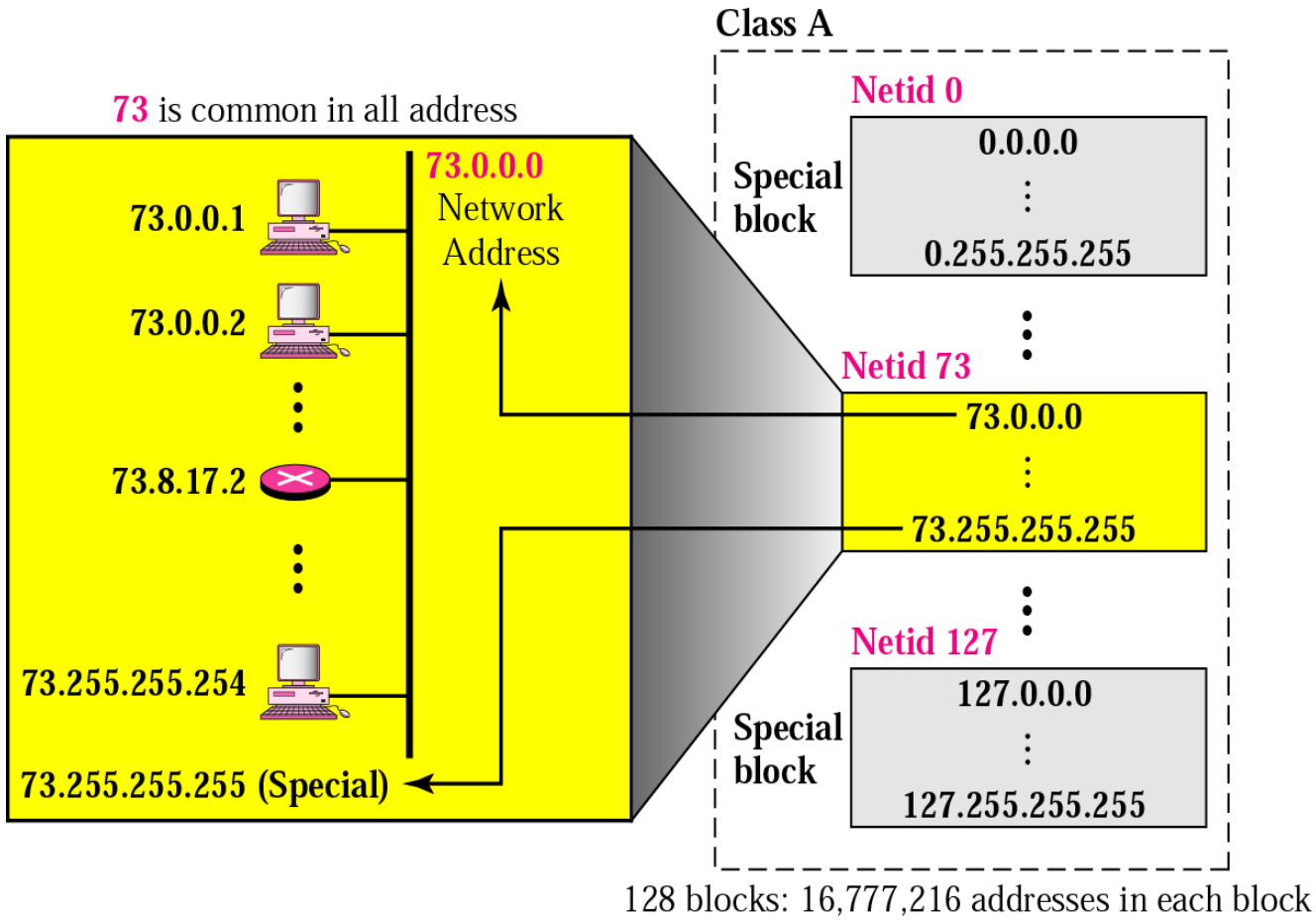
Solution

a. The first byte is 227 (between 224 and 239); the class is D.
b. The first byte is 252 (between 240 and 255); the class is E.
c. The first byte is 134 (between 128 and 191); the class is B.

Netid and hostid

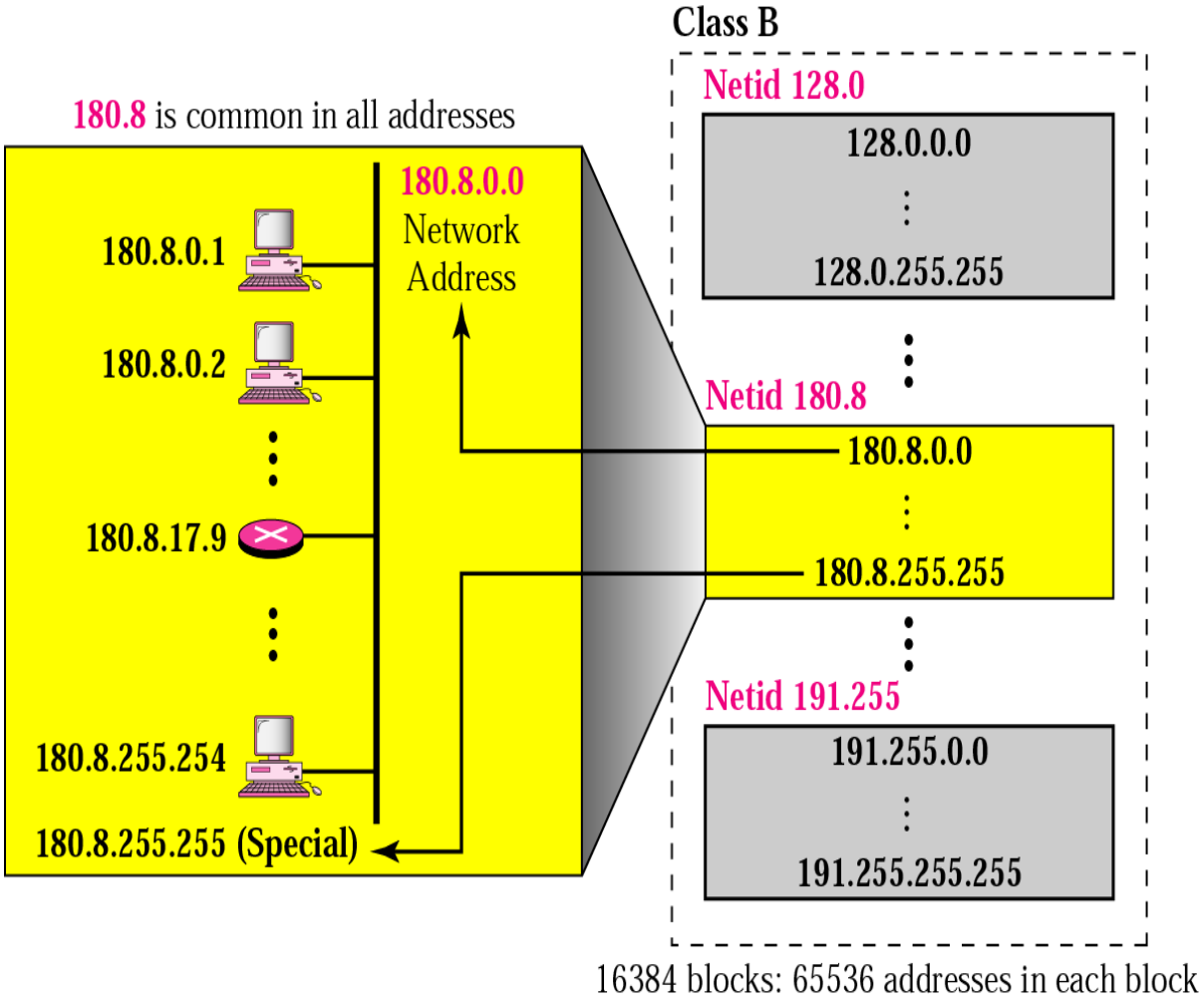


IP Addresses - Class A



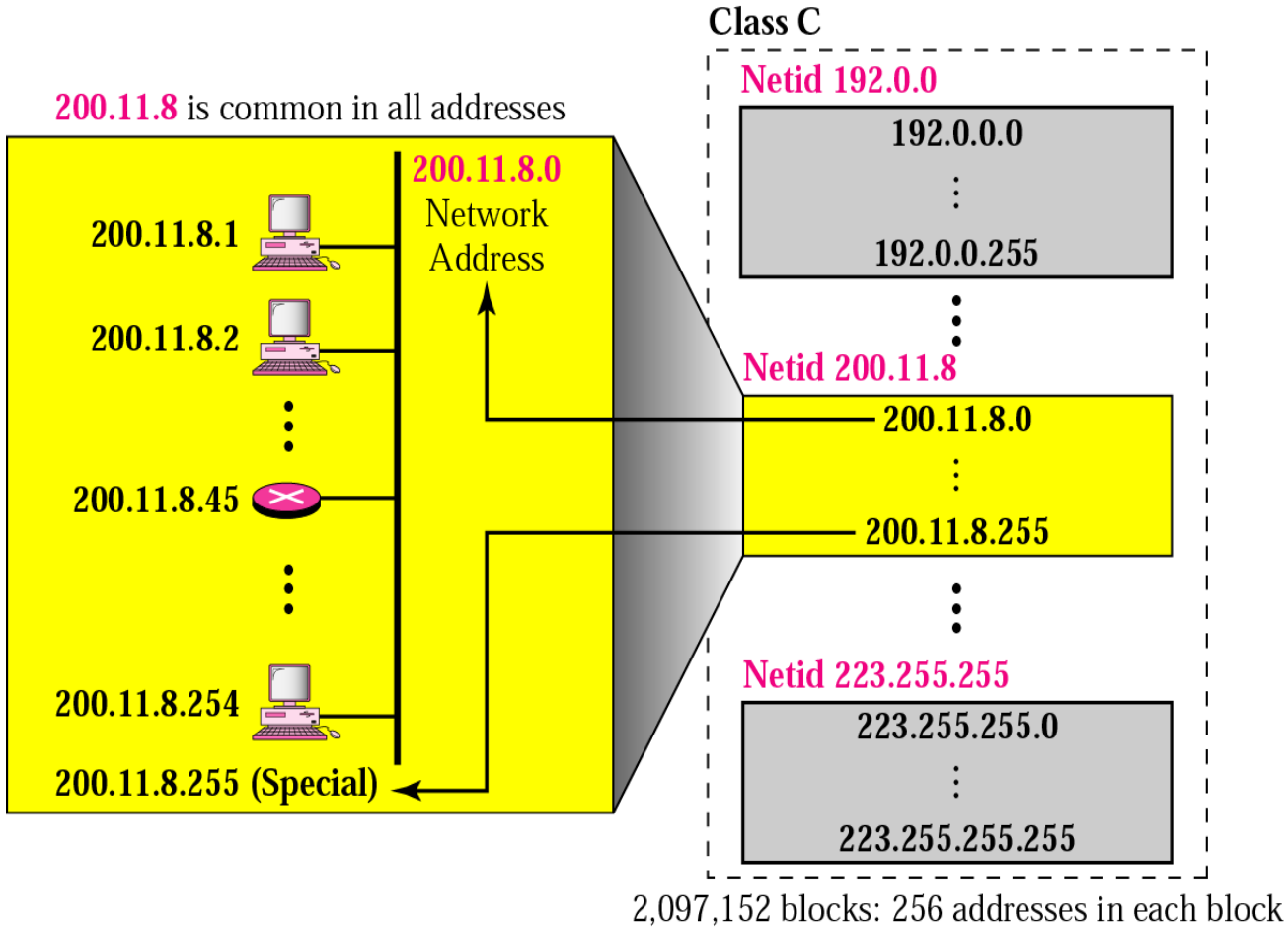
- Start with binary 0
- All 0 reserved
- 01111111 (127) reserved for loop back
- Range 1.x.x.x to 126.x.x.x
- All allocated
- Millions of class A addresses are wasted

IP Addresses - Class B



- Start 10
- Range 128.x.x.x to 191.x.x.x
- Second Octet also included in network address
- 2^{14} = 16,384 class B addresses
- All allocated
- Many class B addresses are wasted

IP Addresses - Class C



- Start 110
- Range 192.x.x.x to 223.x.x.x
- Second and third octet also part of network address
- 2^{21} = 2,097,152 addresses
- Nearly all allocated
- The number of addresses in class C is smaller than the needs of most organizations

IPv4 Network address

- In classful addressing, the network address is the one that is assigned to the organization
- A network address is different from a netid. A network address has both netid and hostid, with 0s for the hostid

Example of Network Address

Example 5

Given the address 23.56.7.91, find the network address.

Solution

The class is A. Only the first byte defines the netid. We can find the network address by replacing the hostid bytes (56.7.91) with 0s. Therefore, the network address is 23.0.0.0.

Example of Network Address

Example 6

Given the address 132.6.17.85, find the network address.

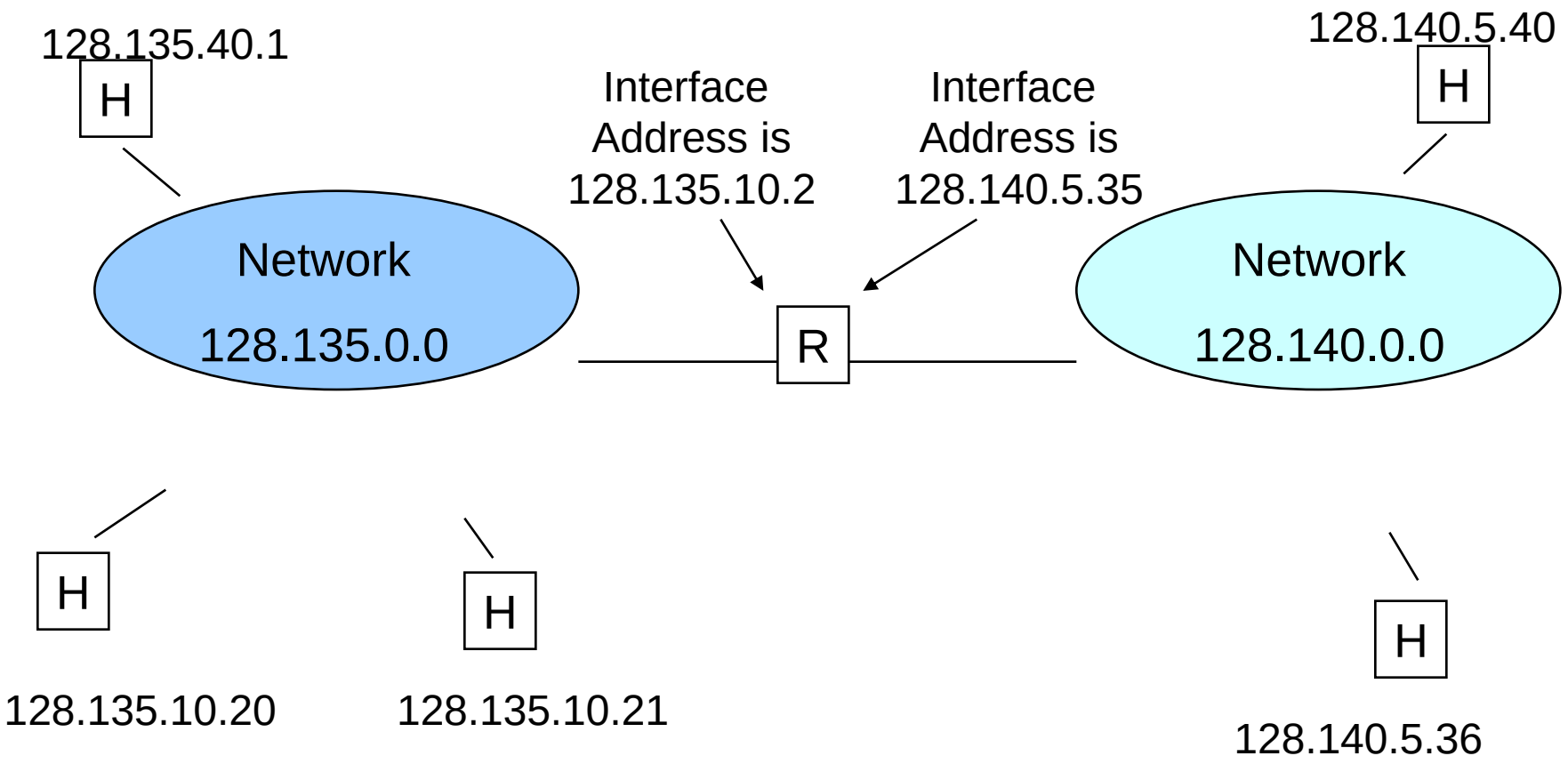
Solution

The class is B. The first 2 bytes defines the netid. We can find the network address by replacing the hostid bytes (17.85) with 0s. Therefore, the network address is 132.6.0.0.

Private IP Addresses

- Specific ranges of IP addresses set aside for use in private networks (RFC 1918)
- Use restricted to private internets; routers in public Internet discard packets with these addresses
- Range 1: 10.0.0.0 to 10.255.255.255
- Range 2: 172.16.0.0 to 172.31.255.255
- Range 3: 192.168.0.0 to 192.168.255.255
- Network Address Translation (NAT) used to convert between private & global IP addresses

Example of IP Addressing in a network



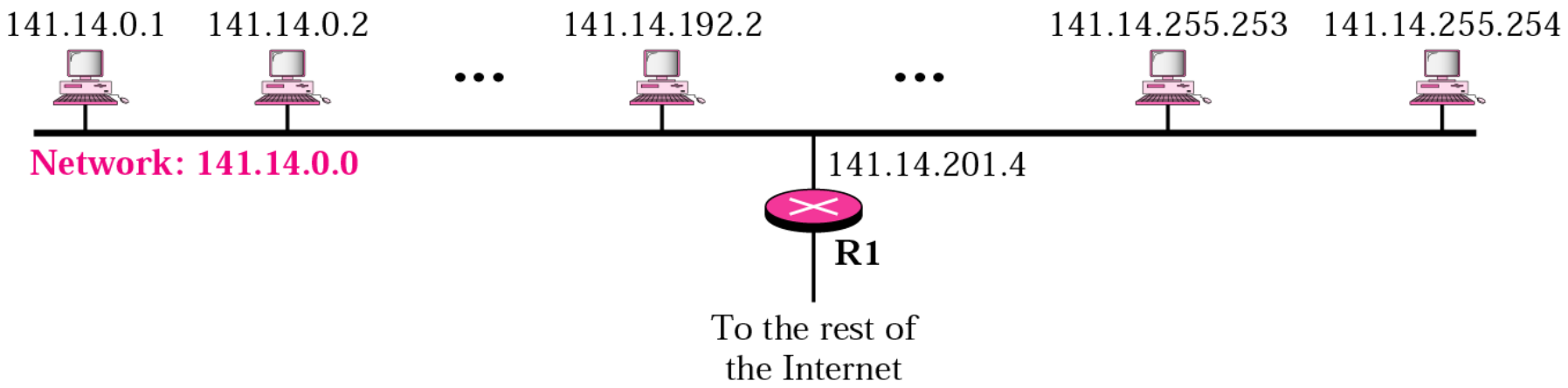
Address with host ID=all 0s refers to the network

Address with host ID=all 1s refers to a broadcast packet

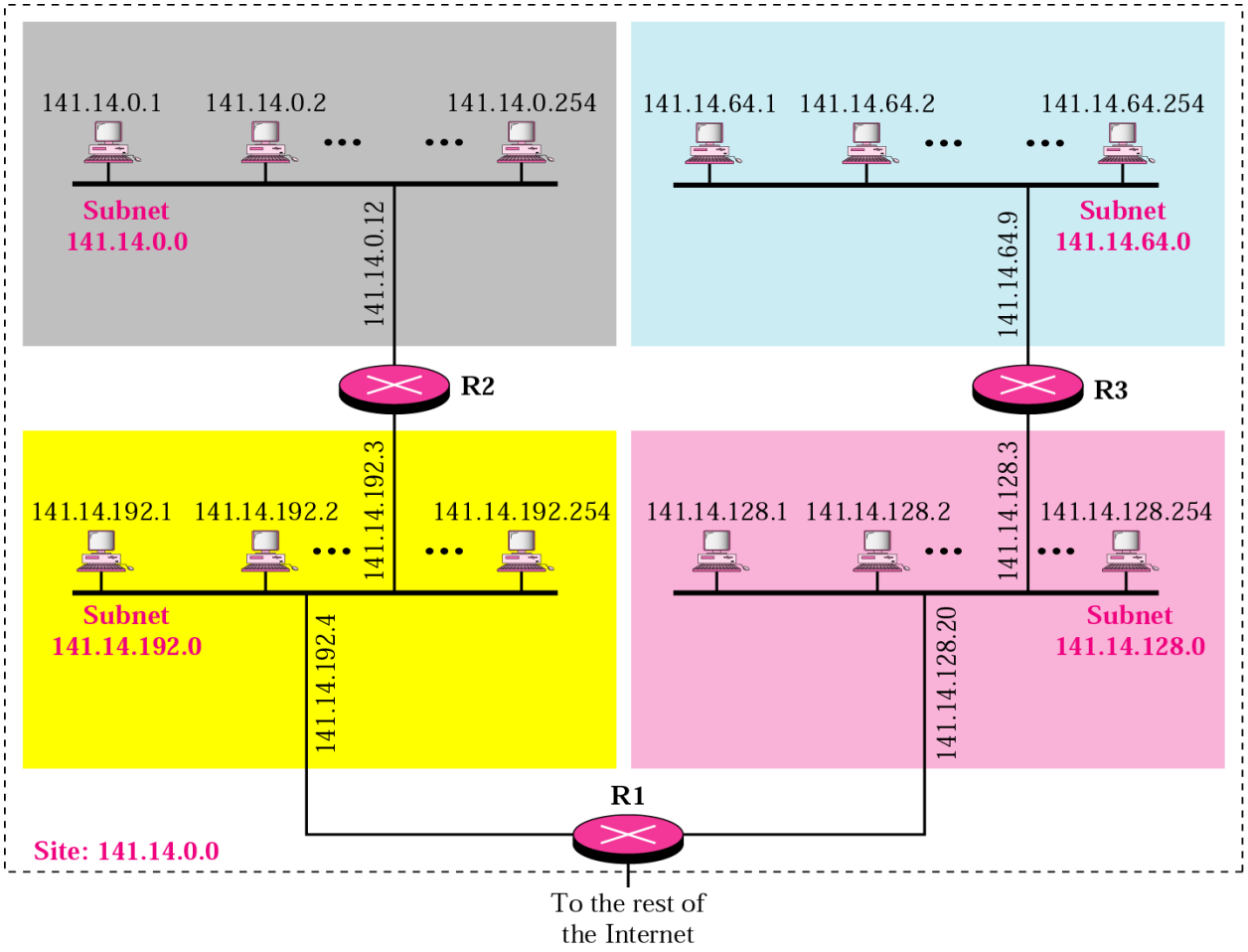
R = router

H = host

A network with two levels of hierarchy



A network with three levels of hierarchy (subnetted)



- Subnet addressing introduces another hierarchical level
- Transparent to remote networks
- Simplifies management of multiplicity of LANs
- Masking used to find subnet number

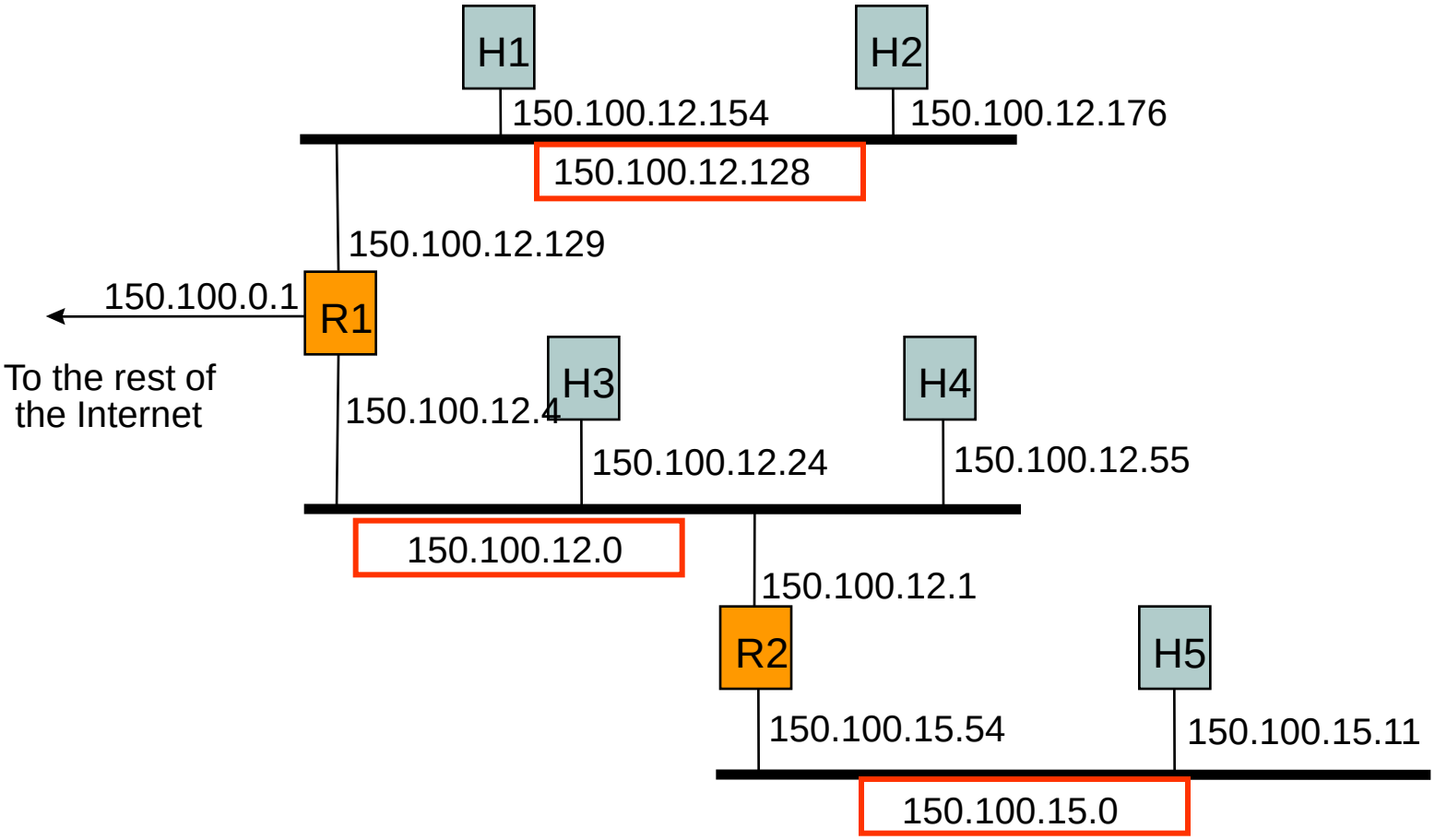
Default Mask

Class	*In Binary*	*In Dotted-Decimal*	*Using Slash*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 111111111 11111111 00000000	255.255.255.0	/24

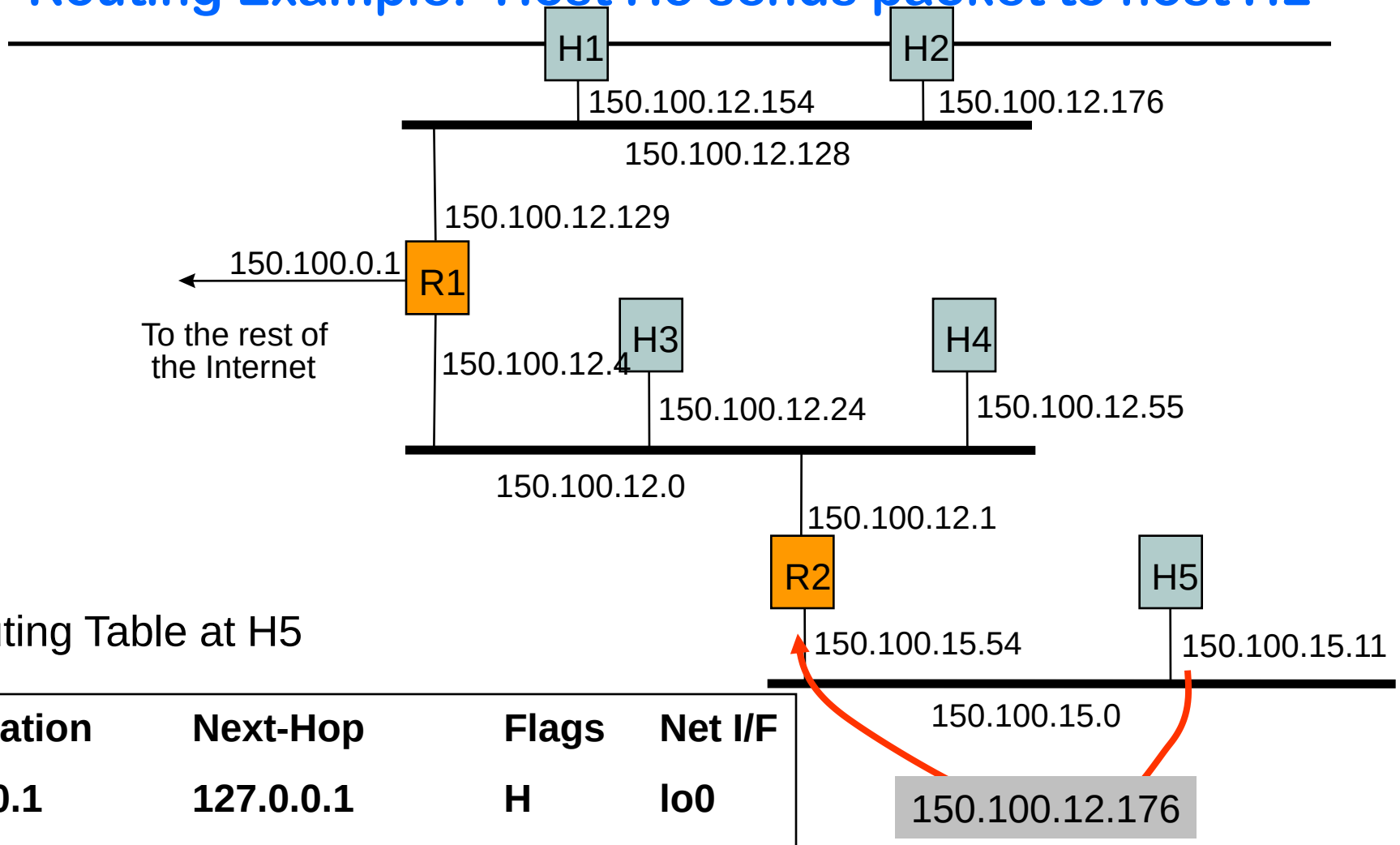
Subnetting Example

- Organization has Class B address (16 host ID bits) with network ID: 150.100.0.0
- Create subnets with up to 100 hosts each
  - 7 bits sufficient for each subnet
  - 16-7=9 bits for subnet ID
- Apply subnet mask to IP addresses to find corresponding subnet
  - Example: Find subnet for 150.100.12.176
  - IP add = 10010110 01100100 00001100 10110000
  - Mask = 11111111 11111111 11111111 10000000
  - AND = 10010110 01100100 00001100 10000000
  - Subnet = 150.100.12.128
  - Subnet address used by routers within organization

Subnet Example



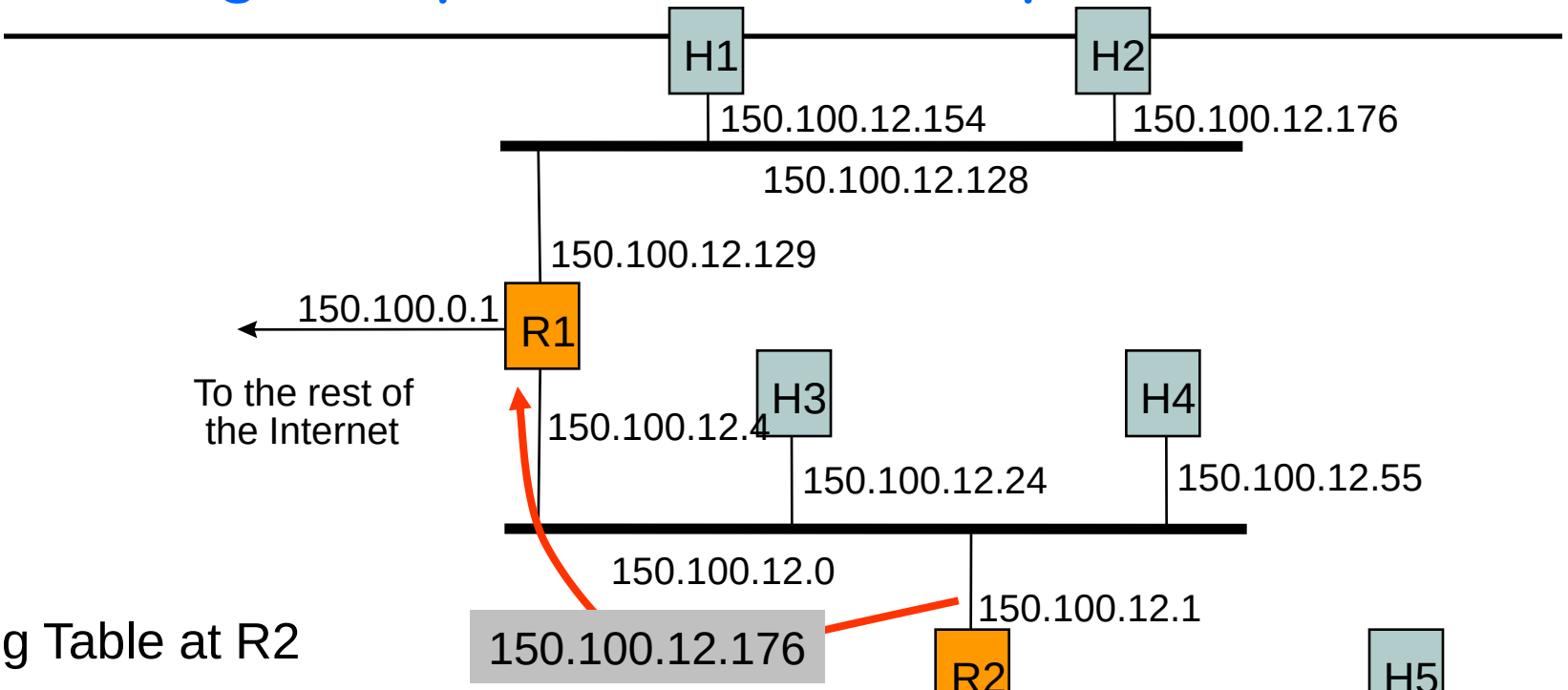
Routing Example: Host H5 sends packet to host H2



Routing Table at H5

Destination	Next-Hop	Flags	Net I/F
127.0.0.1	127.0.0.1	H	lo0
default	150.100.15.54	G	emd0
150.100.15.0	150.100.15.11		emd0

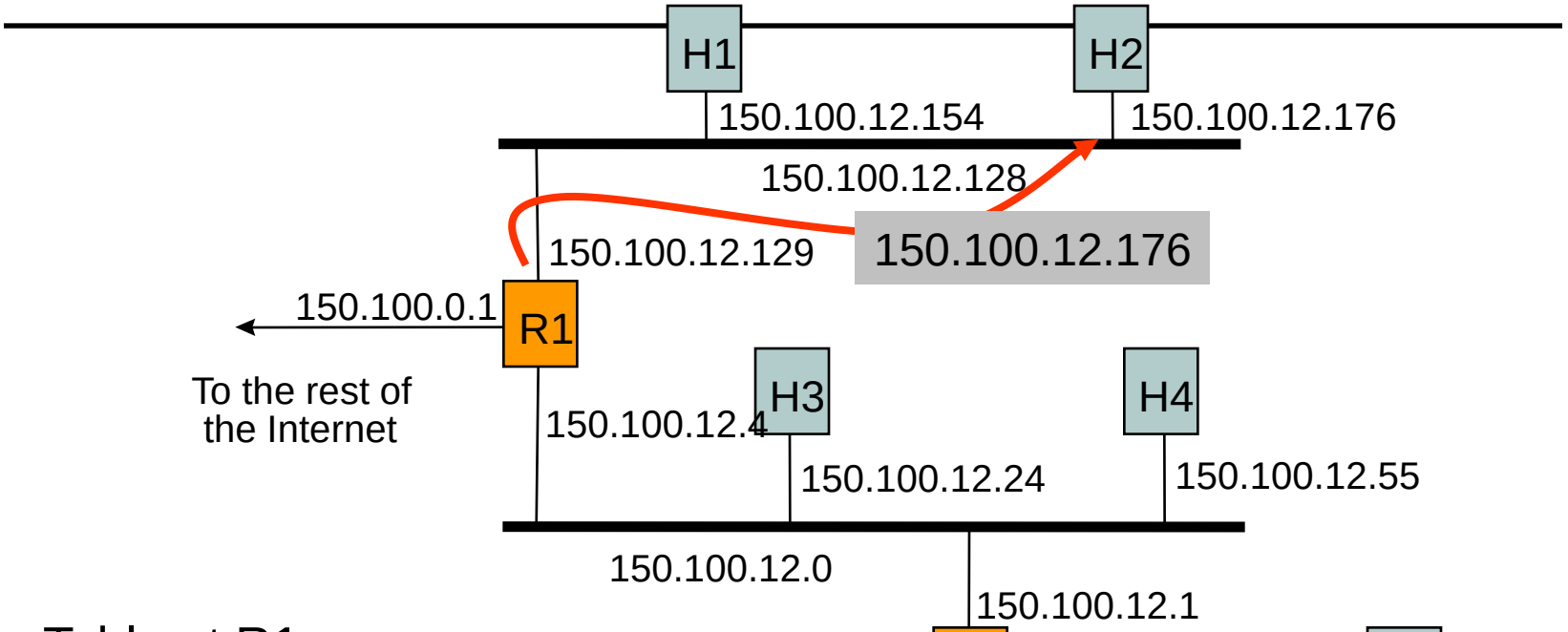
Routing Example: Host H5 sends packet to host H2



Routing Table at R2

Destination	Next-Hop	Flags	Net I/F
127.0.0.1	127.0.0.1	H	lo0
default	150.100.12.4	G	emd0
150.100.15.0	150.100.15.54		emd1
150.100.12.0	150.100.12.1		emd0

Routing Example: Host H5 sends packet to host H2



Routing Table at R1

Destination	Next-Hop	Flags	Net I/F
127.0.0.1	127.0.0.1	H	lo0
150.100.12.176	150.100.12.176		emd0
150.100.12.0	150.100.12.4		emd1
150.100.15.0	150.100.12.1	G	emd1

Limitations of IPv4

- In the 1990, two problems became apparent
  - IP addresses were being exhausted
  - IP routing tables were growing very large
- IP Address Exhaustion
  - Extended use of TCP/IP
  - Network addresses used even if not connected to Internet
  - Single address per host
  - Class A, B, and C address structure inefficient
    - Class B too large for most organizations, but future proof
    - Class C too small
    - Rate of class B allocation implied exhaustion by 1994
- Short-term solution:
- Classless Interdomain Routing (CIDR), RFC 1518
- New allocation policy (RFC 2050)
- Private IP Addresses set aside for intranets
- Long-term solution: IPv6 with much bigger address space

IP v6 - Version Number

- IP v 1-3 defined and replaced
- IP v4 - current version
- IP v5 - streams protocol
- IP v6 - replacement for IP v4
  - During development it was called IPng
  - Next Generation

IPv6 RFCs

- 1752 - Recommendations for the IP Next Generation Protocol
- 2460 - Overall specification
- 2373 - addressing structure
- others (find them)
- www.rfc-editor.org

IPv6 Enhancements

- Expanded address space
  - 128 bit. 128 bits can support up to 3.4×10^{38} hosts
- Improved option mechanism
  - Separate optional headers between IPv6 header and transport layer header
  - Most are not examined by intermediate routes
    - Improved speed and simplified router processing
    - Easier to extend options
- Address auto configuration
  - Dynamic assignment of addresses

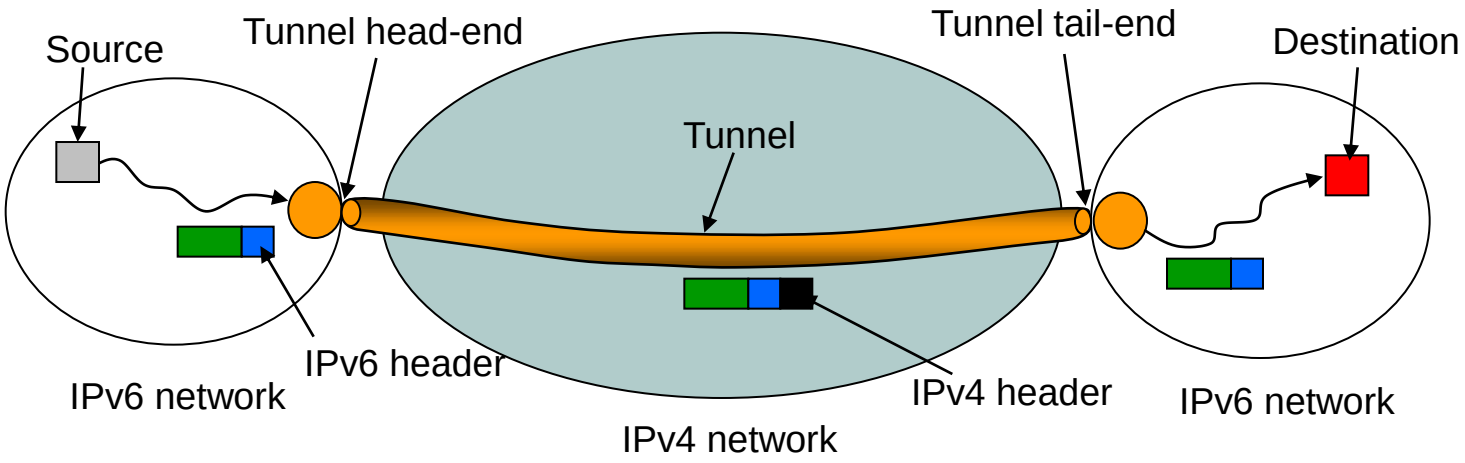
IPv6 Enhancements

- Increased addressing flexibility
  - Any cast - delivered to one of a set of nodes
  - Improved scalability of multicast addresses
- Support for resource allocation
  - Replaces type of service
  - Labeling of packets to particular traffic flow
  - Allows special handling
  - e.g. real time video

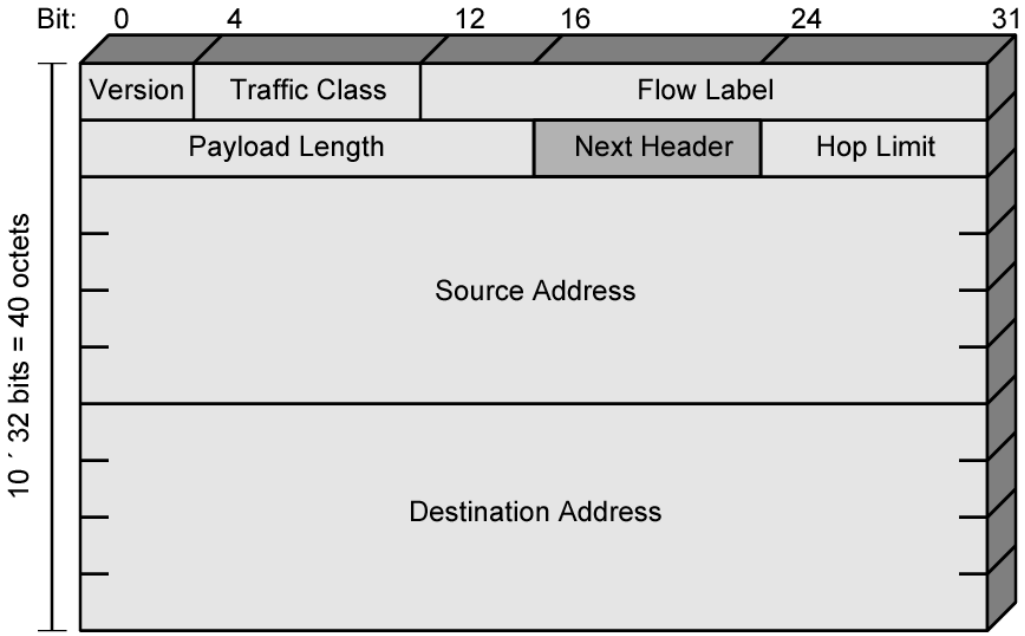
Migration from IPv4 to IPv6

- Gradual transition from IPv4 to IPv6
- Dual IP stacks: routers run IPv4 & IPv6
  - Type field used to direct packet to IP version
- IPv6 islands can tunnel across IPv4 networks
  - Encapsulate user packet insider IPv4 packet
  - Tunnel endpoint at source host, intermediate router, or destination host
  - Tunneling can be recursive

Migration from IPv4 to IPv6 -Tunneling



IP v6 Header



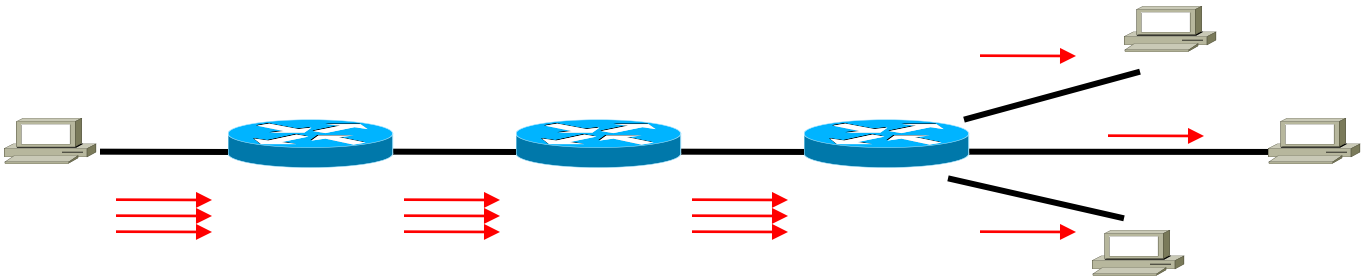
- Version
  - 6
- Traffic Class
  - Classes or priorities of packet
  - Still under development
  - See RFC 2460
- Flow Label
  - Used by hosts requesting special handling
- Next Header
  - Identifies type of header
    - Extension or next layer up
- Source &Destination address
- Payload length
  - Includes all extension headers plus user data

Types of address

- Several address types
  - Unicast
    - An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
  - Multicast
    - An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.
  - Anycast:
    - An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).
- Specified in the the v6 address architecture RFC.

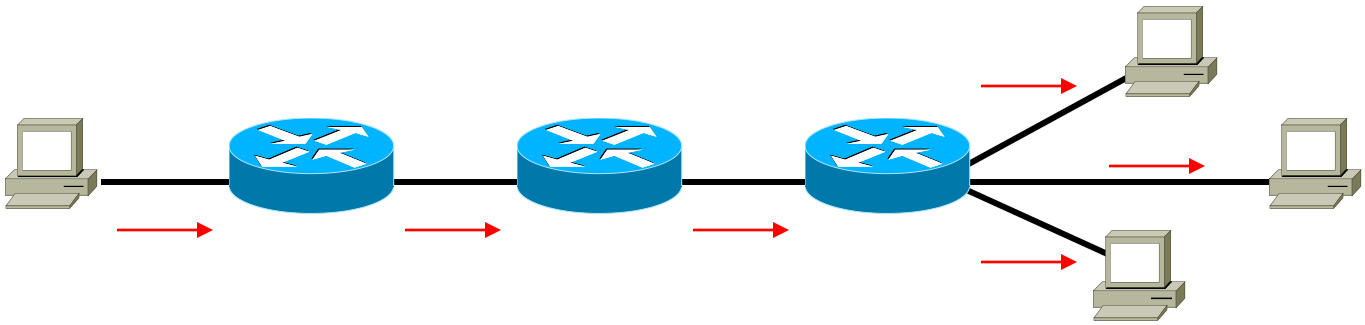
Unicast Communication (1:1)

- One packet for each receiver



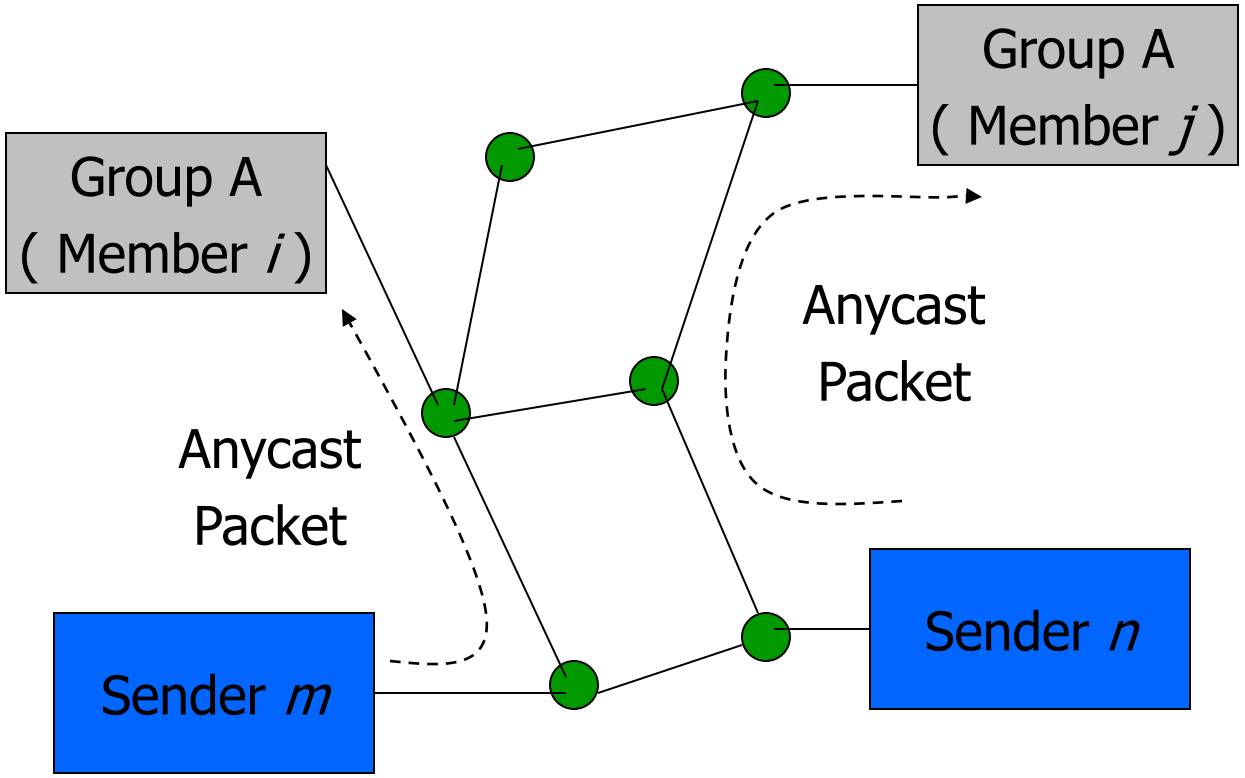
Multicast Communication (1:n)

- One packet to many receivers
  - Routers replicate the packet
  - Like mailing lists
    - One email to many receivers



What is Anycast?

- Anycast (RFC 1546): target many, but get the "nearest" or "best„ according to a defined routing metric
- Application: service discovery & host autoconfiguration
- EX: replicated FTP server, mirror web server



Summary

- In this lecture, we have
  - Reviewed Internetworking
  - Looked at IPv4 format
  - Introduced IPv6
  - Understood the differences between IPv4 and IPv6 and need for IPv6
  - Understood anycasting/multicasting

Next Time

- We will know about
  - Physical Aspects of Data Communications
  - Data Encoding
- Suggested Reading:
  - Chapter 3,4,5 (Stallings)